REMARKS

Claim 1 was pending in the application and has been rejected. Applicant has canceled claim 1 and added new claims 25-30. Support for the new claims can be found in Applicant's disclosure as published in United States Patent Application Number 2007/0094722, specifically in paragraphs [0007], [0013], [0022], [0023], and [0025]. Applicant respectfully requests reconsideration.

CLAIM REJECTIONS UNDER 35 USC §103

The Office Action rejected claim 1 under 35 USC 103(a), as being unpatentable over Copeland (US Patent 7,290,283) in view of Ricciulli (US Patent 6,473,405).

Claim 1 has been canceled and replaced with new independent claims 25 and 30. Claim 25 takes the perspective of the intrusion detection system and claim 30 takes the perspective of the disinfection server. The rejection of claim 1 will be addressed with respect to new claims 25 and 30 and their dependent claims.

The Office Action alleges that Copeland teaches the claimed element of "spoofing replies to requests contained in the data traffic identified" and points to Copeland at Col. 7, lines 55-67. Applicant disagrees with the Examiner's contention that Copeland teaches spoofing and points to the cited portion of Copeland for support: "Consequently, a port profiling engine will monitor flows to determine legitimate flows in which data is transferred. In accordance with an aspect of the invention, the port profiling engine **155** works by assigning data packets **101** to various legitimate flows. A legitimate flow is a communication in which data is sent and acknowledged. Port scans and some other illegitimate flows typically do not send data with the

packets **101**, or if they do, the packets are usually rejected by a TCP "Reject" packet of a ICMP "Unavailable" packet. The engine **155** collects port information associated with each flow and stores this information in a database **160**."

Clearly, Copeland differs from claims 25 and 30 in that Copeland discusses a "method for detecting unauthorized network usage based upon port profiling. This novel detection system does not require a known signature database of known attacks. Instead, the monitoring system inspects all inbound and outbound activity and identifies new services that are not listed on that host's service profile." See Copeland, Col. 3, lines 43-48. Copeland's port profiling method differs from spoofing. Spoofing in this context means masquerading as a legitimate response to a request. In contrast, port profiling is defined by Copeland at Col. 1, lines 46-49 as: "a detection system that monitors network activity by comparing network activity with a prestored profile and identifies suspicious port activity that may indicate unauthorized network activity." Copeland's port profiling method teaches away from the claimed element of spoofing a response in order to determine if the request is a network attack.

Copeland further teaches away from claims 25 and 30 in that Copeland not only does not use spoofing, but Copeland does not make use of signature comparison. See Col. 4, lines 63-65: "Port profiling does not rely on analyzing the data of packets for signatures of known attacks." Likewise, Ricciulli is silent on both spoofing and signature comparison.

As to claim 30, Copeland does not teach the use of a disinfection server to receive an alert message comprising signatures of known attacks, sending a warning message, and providing a report. Ricciulli also does not teach these claim elements. Therefore, independent

claims 25 and 30 are patentable over the cited references.

Claim 26 is dependent on claim 25 which is patentable over the cited references; therefore claim 26 is patentable.

Claim 27 requires, in addition to the limitations of its parent claim, a requirement for signatures stored in memory, which requirement is not taught by either Copeland or Ricciulli.

Claim 28 also requires, in addition to the limitations of its parent claim, a requirement for signatures stored in memory. Therefore, claim 28 is also patentable over the cited references.

Claim 29 requires, in addition to the limitations of its parent claim, listening only for the unassigned data traffic, which limitation is not taught by either cited reference. Therefore, claim 29 is patentable over the cited references.

For the foregoing reasons, Applicant respectfully requests allowance of the pending claims 25-30.

Respectfully submitted,

/Michael J. Buchenhorner/

Michael J. Buchenhorner
Reg. No. 33,162

Date: November 20, 2008

Michael Buchenhorner, P.A.
8540 S.W. 83 Street
Miami, Florida 33143
(305) 273-8007 (voice)
(305) 595-9579 (fax)